UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/700,656	02/14/2001	Harald Vater	JEK/VATER	7577

7590 08/16/2012

Bacon & Thomas
Fourth Floor
625 Slaters Lane
Alexandria, VA 22314-1176

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2492	

MAIL DATE	DELIVERY MODE
08/16/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte HARALD VATER, HERMANN DREXLER, and
ERIC JOHNSON

Appeal 2012-000793
Application 09/700,656
Technology Center 2400

Before JEFFREY S. SMITH, BRUCE R. WINSOR, and JENNIFER S. BISK, *Administrative Patent Judges*.

BISK, *Administrative Patent Judge*.

DECISION ON APPEAL

DECISION ON APPEAL

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's non-final rejection of claims 26-33 and 42, which are all of the remaining claims. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

STATEMENT OF THE CASE

Appellants' invention relates to protecting secret data stored in a memory of a semiconductor chip of a data carrier. *See generally* Spec. Claim 26, reproduced below with emphases added, is representative of the claimed subject matter:

> 26. A method for protecting secret data stored in a memory of a semiconductor chip of a data carrier, said secret data serving as input data for one or more operations executed on the semiconductor chip, the execution of the one or more operations causing signals detectable from outside of the data carrier, the signals being dependent on the one or more operations and on the input data for the one or more operations, said method comprising the steps of:
>
> - falsifying the input data by combination with auxiliary data (Z) *before execution of the one or more operations (f) on the semiconductor chip*,
> - executing said one or more operations (f) on the semiconductor chip,
> - retrieving an auxiliary function value ($f(Z)$) from said memory of said semiconductor chip of the data carrier,
> - combining the output data determined by said executing of the one or more operations (f) with said auxiliary function value ($f(Z)$) in order to compensate for the falsification of the input data,
> - wherein the auxiliary function value ($f(Z)$) was previously determined by execution of the one or more operations (f) with

the auxiliary data (*Z*) as input data in *safe surroundings* and *store along with the auxiliary data (Z) in the memory of the semiconductor chip* of the data carrier.

THE REJECTION

Claims 26-33 and 42 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kocher (US 2002/0124178 A1; Sep. 5, 2002) and Cordery (US 5,655,023; Aug. 5, 1997). Ans. 4-6.

THE CONTENTIONS

The Examiner finds that Kocher discloses all the limitations of representative claim 26 except "determining the auxiliary value previously and in safe surroundings." Ans. 4-5. The Examiner cites to Cordery as disclosing this limitation. In addition, the Examiner explains that it would have been obvious to one of ordinary skill in the art at the time of the invention "to modify the method of Kocher to include pre-computation and safe storage of secret function values [disclosed in Cordery] in order to protect the encryption algorithm and secret key used." Ans. 5 (citing Cordery, col. 3, ll. 11-13).

Appellants do not dispute that all the steps of representative claim 26 are disclosed by the prior art (App. Br. 4, 16-17), but argues that "the ***combination*** of the first, second, and fourth steps with the third and fifth steps . . . is not disclosed in the prior art" and it would not have been obvious to a person of ordinary skill in the art that the two references could or should be combined. App. Br. 4; *See generally* App. Br. 6-18; Reply Br. 2-8.

ISSUE

Is the Examiner's reason to combine the teachings of Kocher and Cordery supported by articulated reasoning with some rational underpinning to justify the Examiner's obviousness conclusion?

ANALYSIS

We do not find Appellants' arguments persuasive. The relevant inquiry is whether the claimed subject matter would have been obvious to those of ordinary skill in the art in light of the combined teachings of the references. *See In re Keller*, 642 F.2d 413, 425 (CCPA 1981). The Examiner's findings regarding what Kocher and Cordery would teach a person of ordinary skill in the art are reasonable. Ans. 4-6; 10-14; *see In re Mouttet*, --- F.3d ---, 2012 WL 2384056, at *4 (Fed. Cir. 2012) ("[a] reference may be read for all that it teaches, including uses beyond its primary purpose."). Appellants provide no persuasive evidence to rebut these findings. Mere assertions to that effect are not persuasive. *See Estee Lauder Inc. v. L'Oreal, S.A.*, 129 F.3d 588, 595 (Fed. Cir. 1997) ("'[A]rguments of counsel cannot take the place of evidence lacking in the record.'" (citation omitted)).

Further, most of Appellants' arguments, directed to whether the implementations described in the two references could or would be combined by a person of ordinary skill in the art at the time of the invention, are irrelevant to the Examiner's position which is not based on physically combining the references, but rather what the references' collective teachings would have suggested to ordinarily skilled artisans. *See* Ans. 6-19. We see no error in this position, for "[i]t is well-established that a determination of obviousness based on teachings from multiple references

does not require an actual, physical substitution of elements." *In re Mouttet*, --- F.3d ---, 2012 WL 2384056, at *5 (Fed. Cir. 2012) (citing *In re Etter*, 756 F.2d 852, 859 (Fed. Cir. 1985) (en banc) (noting that the criterion for obviousness is not whether the references can be physically combined, but whether the claimed invention is rendered obvious by the teachings of the prior art as a whole)).

In short, modifying the method of protecting secret information disclosed in Kocher using pre-calculated and stored secret function values as suggested by Cordery merely predictably uses prior art elements according to their established functions—an obvious improvement. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). We therefore find the Examiner's reason to combine the teachings of the cited references supported by articulated reasoning with some rational underpinning to justify the Examiner's obviousness conclusion.

For the above reasons, the obviousness rejection of claim 26, and claims 27-33 and 42, which were not argued separately (App. Br. 5), is sustained.

DECISION

The Examiner's decision rejecting claims 26-33 and 42 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

rwk